IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 10/782,678
Filing Date ..... February 19, 2004
Inventorship ..... Zigmond
Applicant ..... Microsoft Corp.
Group Art Unit 3621
Examiner ..... Agwumezie, Charles C.
Old Docket No. MS1-1838US
Attorney's Docket No. MS-306815.01
Title: Persistent License for Stored Content

To: The Honorable Commissioner for Patents
Mail Stop Appeal Brief- Patents
PO Box 1450
Alexandria, Virginia 22313-1450

From: William J. Breen III (Tel. 509.755.7253; Fax 509.755.7252)
Customer No. 69316

REPLY OF APPELLANT

This is a reply to the Examiner's Answer Dated July 9, 2007.

ARGUMENT

Claims 1-42 satisfy the requirements of 35 U.S.C. § 102(b) and therefore are not unpatentable over Mohammed.

Regarding **Claim 1,** the Examiner in the *Examiner's Answer* still equates a key ID with the key of Claim 1 that is formed in the request by the client. For example, the Examiner asserts the following which was excerpted from page 19 of the *Examiner's Answer*:

> In response, Examiner respectfully disagrees and submits that Mohammed discloses all of the recited features of claim 1 as shown in the rejection above and on the attached chart. Mohammed further shows the communication of an encrypted key from the client, which is then decrypted by the licensing server and communicated back to the client to access the content (0016; 0017). As shown in the chart, Mohammed made it clear that:
>
> "A license request also includes an identification of the digital content for which a license is requested and a key ID that identifies the decryption key associated with the requested digital content."

As shown in the above excerpt, a "key ID" is communicated and not a "key". The underlining provided by the Examiner, while creative, still does not disclose the claimed subject matter. This is further supported by the "Appeal Chart", in which the Examiner asserts that "the persistent license includes a key that is encrypted such that the key is not accessible by the client" with "the request includes Key ID that identifies the decryption key

(KD) (0017; 0151)". *See Examiner's Answer, Appeal Chart.* As is readily apparent, a key and an identifier of a key are clearly not the same. Further, the key that is included in the request of claim 1 is the key that is received, which is also clearly not the case in Mohammed.

As previously stated, Mohammed does not show the communication of an encrypted key **from the client**, which is then decrypted by the licensing server and **communicated back to the client** to access the content. Although Mohammed does disclose communication of a key, this is not the key that is used to decrypt the content as claimed in claim 1, but rather is used to encrypt another key for communication to the client. It is readily apparent from a reading of Mohammed that this other key that is encrypted is therefore not the original key that was communicated to the licensing server in Mohammed. Rather, the public key communicated by the client machine of Mohammed is accessible by the client and is communicated to the license server to encrypt the decryption key. Therefore, the public key of Mohammed is also not communicated back to the client, as the client already has the public key that is accessible by the client. Further, Mohammed does not disclose that the public key is not accessible by the client machine as recited in Claim 1. Therefore, it is respectfully submitted that Claim 1 is allowable.

With regards to **Claim 11**, a persistent license is received "that includes a key that is encrypted; the key, when decrypted, provides access to the encrypted content", "the client is not configured to decrypt the key from the persistent license". The Examiner, however,

again asserts the same sections of Mohammad as described above that disclose communication of a "Key ID" and not a "Key" as recited. For these and other previously recited reasons, a *prima facie* case of anticipation has also not been established for this claim.

With regards to **Claim 17,** the Examiner again mixes elements in the rejection. For example, Claim 17 recites first and second requests. The first request "is for storing encrypted content". The second request is "to access the encrypted content" and "includes the persistent license" that "includes a boundary key" as recited in Claim 17. In the Appeal Chart, however, the Examiner asserts obtaining a new at the license server (e.g., "No Valid license? Acquire license 16 from License server 24 (see fig. 5)" and therefore this new license is not "the persistent license" as in claim 17 that includes the boundary key that is communicated in the second request. Rather, Mohammed as asserted by the Examiner obtains this license from the license server itself, and not from the client. For these and other previously recited reasons, a *prima facie* case of anticipation has also not been established for this claim.

Regarding **Claims 23 and 33,** the Examiner again asserts that an ID is the same as a key, but in this case asserts a different ID than that asserted in the rejection of Claim 1. For example, in the rejection of Claim 23 the Examiner asserts "includes the persistent license" as a "User id (0017)". *See Appeal Chart.* In the rejection of Claim 33, the Examiner asserts "a persistent license having a key that is encrypted" as a "User id having a Key ID". *See Appeal Chart*. As previously stated with respect to Claim 1, however, this User ID is not a

key, nor is a User id having a Key ID. For these and other previously recited reasons, a *prima facie* case of anticipation has also not been established for these claims.

All other claims are also allowable for the reasons previously recited in the Appeal Brief, and therefore will not be repeated here for the sake

CONCLUSION

The Applicant respectfully considers this application to be in condition for allowance and respectfully requests the Board to overturn the final rejection and that the Examiner pass this application to allowance.

Dated this 29th day of August, 2007.

Respectfully submitted,

/William J. Breen, III #45,313/
WILLIAM J. BREEN, III
Attorney for Applicant
Registration No. 45,313

Sadler, Breen, Morasch and Colby, p.s.
422 W. Riverside Ave., Suite 424
Spokane, WA 99201
509.755.7253

APPENDIX: CLAIMS ON APPEAL

1. (original): A method comprising:

forming a request by a client to access encrypted content, wherein:

the request includes a persistent license for communication to a licensing server; and

the persistent license includes a key that is encrypted such that the key is not accessible by the client; and

receiving a license in response to the request, wherein the received license includes the key that is:

accessible by the client; and

for accessing the encrypted content.

2. (original): A method as described in claim 1, further comprising:

forming an initial request for:

communication to the licensing server; and

storing encrypted content by the client;

receiving the persistent license at the client in response to the initial request; and

storing the encrypted content and the persistent license by the client.

3. (original): A method as described in claim 1, further comprising:

forming an initial request by another client for:

communication to the licensing server; and

storing encrypted content by the other client;

receiving the persistent license at the other client in response to the initial request;

storing the encrypted content and the persistent license by the other client; and

obtaining the persistent license by the client from the other client.

4. (original): A method as described in claim 1, wherein the received license is a boundary license and the key is a boundary key, and further comprising:

decrypting a session license utilizing a client key to obtain a session key;

decrypting the boundary license utilizing the session key to obtain the boundary key;

decrypting a content license utilizing the boundary key to obtain a content key; and

decrypting the encrypted content utilizing the content key.

5. (original): A method as described in claim 4, wherein:

the session license includes access rules for the client for a session initiated between the client and the licensing server;

the boundary license includes access rules for the client for the encrypted content that is within a rights boundary in the encrypted content; and

the content license includes access rules for the client for the encrypted content.

6. (original): A method as described in claim 4, wherein:

the persistent license was encrypted using an asymmetric encryption algorithm; and

the encrypted content, the boundary license, and the content license were encrypted using respective symmetric encryption algorithms.

7. (original): A method as described in claim 1, further comprising:

decrypting a session license utilizing a client key to obtain a session key, wherein the session license includes access rules for a session initiated between the client and the licensing server;

decrypting the received license utilizing the session key to obtain a decrypted boundary license, wherein:

the received license is an encrypted boundary license and the key within the boundary license is a boundary key; and

the boundary license includes access rules for content within a rights boundary in the encrypted content that is at least one of a television program and a television channel;

decrypting a content license utilizing the boundary key to obtain a content key, wherein the content license includes access rules for the encrypted content; and

decrypting the encrypted content utilizing the content key, wherein the encrypted content includes at least a portion of a television broadcast.

8. (original): A method as described in claim 1, wherein the key is for decrypting the encrypted content.

9. (original): A method as described in claim 1, wherein the encrypted content is streamed to the client.

10. (original): One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 1.

11. (original): A method comprising:

forming a request by a client for communication to a licensing server, wherein the request is for storing encrypted content by the client;

receiving a persistent license at the client in response to the request, wherein:

the persistent license includes a key that is encrypted;

the key, when decrypted, provides access to the encrypted content;

the key is configured to be decrypted by the licensing server; and

the client is not configured to decrypt the key from the persistent license; and

storing the persistent license and the encrypted content by the client.

12. (original): A method as described in claim 11, further comprising:

forming a subsequent request by the client to access the stored content, wherein the subsequent request:

is for communication to the licensing server; and

includes the persistent license; and

receiving a second license at the client in response to the subsequent request, wherein:

the second license includes the key; and

the second license is configured to be decrypted by the client such that the client obtains access to the key.

13. (original): A method as described in claim 11, further comprising:

forming a subsequent request by another client to access the stored content, wherein the subsequent request:

is for communication to the licensing server; and

includes the persistent license; and

receiving a second license at the other client in response to the subsequent request, wherein:

the second license includes the key; and

the second license is configured to be decrypted by the other client such that the other client obtains access to the key.

14. (original): A method as described in claim 11, wherein the encrypted content is streamed to the client.

15. (original): A method as described in claim 11, wherein the license includes a certificate for verifying the licensing server by the client.

16. (original): One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 11.

17. (original): A method comprising:

forming a first request for communication to a licensing server, wherein the first request is for storing encrypted content;

receiving a persistent license in response to the request, wherein the persistent license includes a boundary key;

storing the persistent license and the content;

forming a second request to access the encrypted content, wherein the second request includes the persistent license;

sending the second request to the licensing server;

receiving a boundary license in response to the second request, wherein the boundary license includes the boundary key;

decrypting the boundary license using a session key to obtain the boundary key;

decrypting a content license using the boundary key to obtain a content key; and

decrypting the encrypted content using the content key.

18. (original): A method as described in claim 17, wherein the forming of:

the first request is performed by a first client; and

the second request is performed by a second client.

19. (original): A method as described in claim 17, wherein the first and second requests are formed by a client.

20. (original): A method as described in claim 17, further comprising at least one of decoding the decrypted content and outputting the decoded content.

21. (original): A method as described in claim 17, wherein:

the persistent license was encrypted using an asymmetric encryption algorithm; and

the content, the boundary license, and the content license were encrypted using

respective symmetric encryption algorithms.

22. (original): One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 17.

23. (original): A client comprising:

a processor; and

memory configured to maintain:

a persistent license including a key that is encrypted; and

a playback application that is executable on the processor to:

form a request to access encrypted content, wherein the request:

is for communication to a licensing server; and

includes the persistent license;

receive a response to the request that includes the key; and

access the encrypted content utilizing the key.

24. (original): A client as described in claim 23, wherein the key is for decrypting the encrypted content.

25. (original): A client as described in claim 23, wherein:

the memory is further configured to maintain a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

26. (original): A client as described in claim 23, wherein:

the memory is further configured to maintain a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the content license using the key to obtain the content key; and

decrypt the content using the content key.

27. (original): A client as described in claim 23, wherein:

the memory is further configured to maintain a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

28. (original): A client as described in claim 23, wherein:

the memory is further configured to maintain a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the session license using the client key to obtain the session key;

decrypt the boundary license using the session key to obtain the boundary key;

decrypt the content license using the boundary key to obtain the content key; and

decrypt the content using the content key.

29. (original): A client as described in claim 23, wherein the playback application is further executable to:

form an initial request for:

communication to the licensing server; and

storing encrypted content by the playback application;

receive the persistent license in response to the initial request; and

store the encrypted content and the persistent license.

30. (original): A client as described in claim 23, wherein the playback application is further executable to form a request to obtain the encrypted content from another client.

31. (original): A client as described in claim 23, further comprising a tuner configured to receive the encrypted content when streamed over a network.

32. (original): A client as described in claim 23, wherein the license includes a certificate for verifying the licensing server.

33. (original): A system comprising:

a network;

a client including:

a persistent license having a key that is encrypted; and

a playback application that is executable to:

form a request to access encrypted content, wherein the request includes the persistent license;

receive a response to the request that includes the key; and

access the encrypted content utilizing the key; and

a licensing server including a licensing module that is executable to:

receive the request including the persistent license;

decrypt the persistent license to obtain the key; and

form the response that includes the key for communication to the client over the network.

34. (original): A system as described in claim 33, wherein:

the client includes a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

35. (original): A system as described in claim 33, wherein:

the client includes a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the content license utilizing the key to obtain the content key; and

decrypt the content utilizing the content key.

36. (original): A system as described in claim 33, wherein:

the client includes a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

37. (original): A system as described in claim 33, wherein:

the client includes a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the session license utilizing the client key to obtain the boundary key;

decrypt the boundary license utilizing the session key to obtain the boundary key;

decrypt the content license utilizing the boundary key to obtain the content key;

decrypt the content utilizing the content key; and

play the decrypted content.

38. (original): A system as described in claim 33, wherein the key is for decrypting the encrypted content.

39. (original): A system as described in claim 33, wherein the persistent license is encrypted with an asymmetric encryption algorithm and the server includes a server private key for decrypting the persistent license.

40. (original): A system as described in claim 33, wherein the playback application

is further executable to:

form an initial request for:

communication to the licensing server; and

storing encrypted content by the playback application;

receive the persistent license in response to the initial request; and

store the encrypted content and the persistent license.

41. (original): A system as described in claim 33, wherein the playback application is further executable to form a request to obtain the encrypted content from another client.

42. (original): A system as described in claim 33, wherein the encrypted content is streamed to the client over the network.